National Infrastructure Protection Center
CyberNotes

Issue #2001-16 *August 13, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 11 and August 10, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[1]	Unix	ColdFusion Server 4.5.1, 5.0	A Denial of Service vulnerability exists in the 'CFReThrow' tag when it is used on a ColdFusion/Linux server combination.	A temporary workaround is to use the CFTHROW tag.	ColdFusion 'CFReThrow' Tag Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Bugtraq, July 30, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[2]	Windows NT 4.0, Unix	Macromedia ColdFusion Server 4.0, 4.0.1, 4.5, 4.5.1, 4.5.1 SP1&SP2	Multiple vulnerabilities exist in two sample applications, which could let a remote malicious user execute arbitrary commands as a privileged user.	Allaire Macromedia will not be releasing a patch for this issue, instead it is suggested that the CFDOCS directory be removed from production environments. All ColdFusion customers should familiarize themselves with the ColdFusion "Best Security Practices" document available at: http://www.allaire.com/Handlers/index.cfm?ID=16258&Method=Full	ColdFusion Sample Application Command Execution CVE Name: CAN-2001-0535	**High**	Bug discussed in newsgroups and websites.
Apache Group[3]	Windows NT 4.0/2000	Apache 1.0, 1.2, 1.3	A vulnerability exists when a HTTP request containing the URI of a directory is submitted to the server, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Apache Server Address Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
ArGoSoft[4]	Windows 95/98/ME/ NT 4.0/2000	FTP Server 1.2.2.2	A vulnerability exists which could let a malicious user view other users' encrypted passwords. Due to a weak encryption scheme it is possible to decrypt the password using a third party utility.	No workaround or patch available at time of publishing.	FTP Server Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Caldera, Incorporated[5]	Unix	OpenUnix 8.0	A buffer overflow vulnerability exists in some DT utilities, which could let a malicious user execute arbitrary code with privileges of root.	No workaround or patch available at time of publishing.	OpenUnix DT Library Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Windows 95/98/ME/ NT 4.0/2000	Cisco SN 5420 Storage Router 1.1(2), 1.1(3)	Two vulnerabilities exist: a vulnerability in the firmware used with SN 5420 routers exists, which could let a remote malicious user gain unauthorized access and elevated privileges; and a remote Denial of Service vulnerability exists.	Upgrade available at: http://www.cisco.com	Cisco SN Storage Router Developer Shell Unauthorized Access and Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites.
Critical Path[7]	Multiple	InJoin Directory Server 2.0, 2.1, 3.0, 3.1, 4.0	Several potential vulnerabilities exist in the LDAP implementation used in the Critical Path InJoin Directory server, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	InJoin Directory Server LDAP	**High**	Bug discussed in newsgroups and websites.

[2] Internet Security Systems Security Advisory, ISS-092, August 7, 2001.
[3] Bugtraq, August 9, 2001.
[4] Securiteam, July 25, 2001.
[5] Bugtraq, August 2, 2001.
[6] Cisco Security Advisory, Revision 1, July 11, 2001.
[7] CERT® Advisory, CA-2001-18, July 19, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Entrust[8]	Multiple	GetAccess 1.0	A vulnerability exists in the execution of Java class files because input is not validated, which could let a malicious user execute Java class files anywhere on the filesystem.	Patch available at: https://www.entrust.com/support/resources/recentsecuritynotes.htm	GetAccess Remote Arbitrary Java Code Execution	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Eric Raymond[9, 10]	Unix	Fetchmail 5.8- 58.9	Two vulnerabilities exist in both the imap and pop3 code because the input is not verified when used to store a number in an array, which could let a remote malicious user gain access to client systems and execute arbitrary code.	Upgrade available at: http://tuxedo.org/~esr/fetchmail/fetchmail-5.8.17.tar.gz **Debian:** http://security.debian.org/dists/stable/updates/main/	IMAP and POP3 Reply Signed Integer Index	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Francisco Burzi[11]	Unix	Francisco Burzi PHP Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4.1a, 4.4, 5.0, 5.0.1	A vulnerability exists because user-supplied input is not properly validated, which could let a malicious user gain administrative privileges.	No workaround or patch available at time of publishing.	PHP Nuke Remote SQL Query Manipulation	**High**	Bug discussed in newsgroups and websites. This vulnerability is exploitable with a web browser.
GNU[12]	Unix	Findutils 4.0, 4.1	A vulnerability exists when the program reads database files composed in an "old" format, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Findutils Locate Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard[13]	Windows NT 4.0/2000, Unix	JetAdmin 4.0, 4.1.2, 5.1, 5.5, 5.5.177, 5.6, 6.0. 6.1, 6.2	A vulnerability exists because JetDirect devices configured using the JetAdmin web interface do not set a password for Telnet access when the administrator password is chosen, which could let a remote malicious user access the device to cause a Denial of Service, or potentially monitor printer activity to gather information that may be used to compromise systems. Also the admin password is reset when the device is rebooted.	**Workaround:** Set the Telnet password manually.	JetDirect JetAdmin Password	Medium	Bug discussed in newsgroups and websites. There is no exploit required.
Hi Resolution[14]	MacOS 8.6	MacAdministrator 2.0	A vulnerability exists due to the interaction between a previously installed toolkit and MacAdministrator, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	MacAdministrator Hidden Files Disclosure	Medium	Bug discussed in newsgroups and websites.

[8] VulnWatch, July 30, 2001.
[9] Bugtraq, August 10, 2001.
[10] Debian Security Advisor, DSA-071-1, August 10, 2001.
[11] Securiteam, August 8, 2001.
[12] Bugtraq, August 1, 2001.
[13] Bugtraq, August 1, 2001.
[14] Bugtraq, August 9, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
id Software[15]	Multiple	Quake 3 Arena Server 1.29f, 1.29g	A buffer overflow vulnerability exists which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Quake 3 Arena Possible Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Identix[16]	Windows 98/ME	BioLogon Client 2.0, 2.0.1-2.0.3	A vulnerability exists because users who access the host from virtual desktops are not authenticated, which could let a malicious user gain access to the desktop of a locked workstation.	No workaround or patch available at time of publishing.	BioLogon Client Biometric Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit is required.
Linksys[17]	Multiple	EtherFast BEFSR41 Router 1-39, 135-137	A vulnerability exists because passwords for the router and the user ISP account can be viewed in the HTML source code stored on the router.	No workaround or patch available at time of publishing.	EtherFast Router Password HTML Source Revealing	Medium	Bug discussed in newsgroups and websites. There is no exploit is required.
Microsoft[18]	Windows 95/98/ME/ NT 4.0/2000	Windows Media Player 7, 7.1	A buffer overflow vulnerability exists when an unusually long marker is embedded in an .ASF file, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Windows Media Player .ASF Marker Buffer Overflow	Low/**High**	Bug discussed in newsgroups and websites.
Microsoft[19]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.0, 5.01, 5.0.1 SP1&SP2, 5.5, 5.5SP1	A vulnerability exists in the HTML parser feature included in Internet Explorer, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Arbitrary HTML File Execution	**High**	Bug discussed in newsgroups and websites.
Microsoft[20]	Windows 98/98SE	Windows 98, 98SE	A Denial of Service vulnerability exists in the Windows network stack when a large number of extraneous ARP packets are sent to the host.	No workaround or patch available at time of publishing.	Windows ARP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[21]	Windows NT 4.0	Windows NT 4.0, 4.0 SP1-SP6a	A Denial of Service vulnerability exists when the system reboots while being set in 'special mode' using the 'NT4ALL' tool.	No workaround or patch available at time of publishing	Windows NT 4.0 NT4ALL Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[22]	Windows NT 4.0/2000	Outlook 2000	A vulnerability exists when an e-mail message is sent using rich text, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Outlook 2000 Rich Text Format Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit required.

[15] Q30wnerz Advisory v1.0, July 30, 2001.
[16] NTBugtraq, August 2, 2001.
[17] Hypoclear Security Advisory, August 2, 2001.
[18] Bugtraq, August 7, 2001.
[19] Bugtraq, July 27, 2001.
[20] Bugtraq, July 30, 2001.
[21] Hypoclear Security Advisory, August 3, 2001.
[22] Securiteam, August 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[23]	Windows NT 4.0/2000	Windows NT 4.0, 4.0 SP1- SP6a, 2000, 2000 SP1&SP2	A vulnerability exists which could let a malicious user reboot the system by executing a command and pressing F7 <enter> during the command execution.	No workaround or patch available at time of publishing.	Windows NT and 2000 Command Prompt Reboot	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[24]	Windows NT 4.0/2000	Internet Information Server 4.0, 5.0	A vulnerability exists if a remote malicious user connects to a host using HTTPS (typically on port 443) and crafts a specially formed GET request, which could disclose the internal IP address or internal network name to remote attackers.	No workaround or patch available at time of publishing.	IIS Internal IP Address/Internal Network Name Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[25]	Unix	Linux kernel 2.0.x, 2.2.x	A vulnerabililty exists in the 'ip_masq_irc' module, which could let a remote malicious penetrate protected private networks.	Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/ip_masq_irc-2.2.19-dcc_check-3.diff	Linux IRC IP Masquerading Module Arbitrary Firewall Rule Insertion	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[26]	Windows 95/98/ME/ NT 4.0/2000	WhizBang Matrix Screen Saver	A vulnerability exists if the 'Password Protected' checkbox has been enabled, which could let a malicious user bypass it by clicking cancel and pressing arbitrary keys.	No workaround or patch available at time of publishing.	WhizBang Matrix Screen Saver Password Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[27]	Windows 95/98/NT 4.0/2000	Fast Track KaZaA 1.3; Music City Networks Morpheus 1.3	A vulnerability exists in the Media sharing component that could enable a malicious user to view the contents of the folder specified for download files, if file sharing is enabled.	**Workaround:** Disable sharing of files with other KaZaA or Morpheus members	Multiple Vendor File Sharing Application File Disclosure	Medium	Bug discussed in newsgroups and websites.
NetWin[28]	Windows 95/98/NT 4.0/2000, Unix	SurgeFTP 2.0a-2.0f	A vulnerability exists due to weak password hashing, which could let a malicious user obtain the administrator password through brute force cracking.	No workaround or patch available at time of publishing.	SurgeFTP Weak Password Encryption	Medium	Bug discussed in newsgroups and websites.
Oracle Corpora-tion[29]	Unix	Oracle8i 8.0.5	A buffer overflow vulnerability exits in the handling of $ORACLE_HOME by 'otrcrep,' which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Oracle OTRCREP Oracle Home Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

[23] Bugtraq, July 27, 2001.
[24] e-Synergies Security Advisory, August 8, 2001.
[25] RAZOR Advisory, July 30, 2001.
[26] Bugtraq, August 1, 2001.
[27] Bugtraq, July 31, 2001.
[28] Bugtraq, August 4, 2001.
[29] Plazasite Security Advisory, August 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[30]	Unix	Oracle8i 8.0.5, 8.0.6, 8.1.5, 8.1.6	A race condition vulnerability exists in the binary, 'oracle', which could let a malicious user corrupt database files, overwrite existing Oracle binaries, etc.	No workaround or patch available at time of publishing.	Oracle /tmp Race Condition	Medium	Bug discussed in newsgroups and websites. There is no exploit required.
Oracle Corporation[31]	Windows 2000, Unix	Oracle8 8.1.6, 8.1.7, Oracle9i 9.0, 9.0.1	A buffer overflow vulnerability exists when the ORACLE_HOME environment variable is filled with 750 bytes or more, which could let a malicious user gain elevated privileges, including administrative access.	No workaround or patch available at time of publishing.	Oracle DBSNMP Oracle Home Environment Variable Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[32]	Unix	Oracle8 8.0.5, 8.1.5	A vulnerability exists in dbsnmp, which could let a malicious user gain elevated privileges including root access.	Upgrade to 8.1.6 or greater available at: http://otn.oracle.com/software/content.html	Oracle DBSNMP CHOwn Path Environment Variable	**High**	Bug discussed in newsgroups and websites. There is no exploit is required.
Oracle Corporation[33]	Windows 2000	Oracle8 8.1.6, 8.1.7	A input validation vulnerability exists in dbsnmp, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Oracle DBSNMP Oracle Home Environment Variable Changing	**High**	Bug discussed in newsgroups and websites. There is no exploit required.
phpBB Group[34]	Unix	phpBB 1.0.0, 1.2.0, 1.2.1, 1.4.0	An input validation vulnerability exists in some variables in phpBB, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.phpbb.com/download/phpBB-1.4.1.tar.gz	PHPBB Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
phpBB Group[35]	Unix	phpBB 1.4.0, 1.4.1	An input validation vulnerability exists which could let a remote malicious user execute arbitrary SQL queries. This would allow administrative access.	No workaround or patch available at time of publishing.	PHPBB Remote SQL Query Manipulation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
phpMy Admin[36]	Unix	phpMy Admin 2.0-2.0.5, 2.1-2.1.2, 2.2pre1, 2.2rc1-2.2rc3	An input validation error exists in the 'tbl_copy.php' and 'tbl_rename.php' scripts, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	phpMyAdmin Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.

[30] Plazasite Security Advisory, August 2, 2001
[31] Plazasite Security Advisory, August 2, 2001.
[32] Bugtraq, August 1, 2001.
[33] Bugtraq, August 1, 2001.
[34] Bugtraq, August 10, 2001.
[35] VulnWatch, August 3, 2001.
[36] Securiteam, August 1, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Raytheon[37]	Multiple	SilentRunner 1.6.1, 2.0, 2.0.1 ('Knowledge Browser' vulnera-bility)	Multiple buffer overflow vulnerabilities exist in the collector (cle.exe) component due to improper bounds checking on user-supplied passwords, which could let a malicious user execute arbitrary code. An additional buffer overflow vulnerability exists in 'Knowledge Browser' in its processing of HTTP requests, which could let a remote malicious user execute arbitrary code.	Upgrade to 2.0.1 to fix the password buffer overflow vulnerabilities. No workaround or patch available at time of publishing for the 'Knowledge Browser' vulnerability.	Raytheon SilentRunner Multiple Buffer Overflow Vulnerabilities CVE Name: CAN-2001-0636	**High**	Bug discussed in newsgroups and websites.
Roxen[38]	Windows, Unix	Webserver 2.0, 2.1	A vulnerability exists in the way encoded URLs are handled, which could let a remote malicious user execute arbitrary code.	Patch available at: http://download.roxen.com/	Roxen Remote File Access	**High**	Bug discussed in newsgroups and websites.
Ti Kan[39]	Unix	Xmcd 2.6.0, 3.0.0, 3.0.1	A race condition exists in 'cda', which could let a malicious user cause a Denial of Service or gain elevated privileges.	Upgrade available at: http://www.ibiblio.org/tkan/download/xmcd/src/xmcd-3.0.2.tar.gz **SuSE:** ftp://ftp.suse.com/pub/suse/	XMCD Temp Directory Symbolic Link	Low/ Medium	Bug discussed in newsgroups and websites.
Trend Micro, Incor-porated[40]	Windows 3.5/3.5.1/ NT 4.0	InterScan VirusWall for Windows NT 3.51	A vulnerability exists due to the inability to decode certain types of attachments. InterScan is unable to filter or clean the TROJ_SIRCAM.A virus from attachments in electronic mail format (.eml).	Patch available at: http://solutionbank.antivirus.com/solutions/solutionDetail.asp?solutionId=9756	InterScan VirusWall Sircam Virus	Medium	Bug discussed in newsgroups and websites. There is no exploit required.
VMWare, Incor-porated[41]	Unix	VMWare 2.0	A vulnerability exists in the /tmp file, vmware-log.username which could let a malicious user gain sensitive information.	A workaround is to set the TMP environment variable to a safe and/or private location for each user, and in the master environment files on the system.	VMWare TMP Directory License Information	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Wolfram Research[42]	Multiple	Mathematica 4.0, 4.1	Two vulnerabilities exist: a remote Denial of Service vulnerability exists due to incorrectly handled connection requests; and it is possible for remote malicious users to gain arbitrary access to Mathematica licenses.	No workaround or patch available at time of publishing.	Mathematica License Retrieval and Manager Connected Port Denial Of Service	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[37] Internet Security Systems Security Advisory, ISS-091, August 6, 2001.
[38] SecurityFocus, August 2, 2001.
[39] SuSE Security Announcement, SuSE-SA:2001:025, August 3, 2001.
[40] Bugtraq, August 2, 2001.
[41] Bugtraq, July 30, 2001.
[42] Securiteam, August 1, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
World visions Computer Technology [43]	Unix	WvDial 1.4.1, 1.4.2	A vulnerability exists in the default installation configuration file, 'wvdial.conf', which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	WvDial Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit is required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 25 and August 10, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 31 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 10, 2001	Fetchmail-exploit.c	Script which exploits the Fetchmail IMAP and POP3 Reply Signed Integer Index vulnerability.
August 10, 2001	Nmap-2.54beta29.tgz	A utility for port scanning large networks, which supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
August 8, 2001	Rootscanner.pl	A scanner that finds root.exe, the backdoor left by the Code Red II Trojan.

[43] Bugtraq, August 1, 2001.

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 8, 2001	Fmtbuild.htm	Format String Builder includes code and instructions for use of a program which aids in the creation of format string exploits and includes fmtbuilder.c, a small program to help build the strings.
August 8, 2001	Nessus-1.0.9.tar.gz	A multithreaded and plugin-based full featured remote security scanner for Linux, BSD, Solaris and some other systems; it currently performs over 531 remote security checks.
August 5, 2001	Vlad-0.9.2.tar.gz	A freeware, open-source scanner that checks for the common security problems referenced in the SANS Top Ten list of common security problems.
August 5, 2001	**Otrcrep-8.0.5.C**	**Script which exploits the Oracle OTRCREP Oracle Home Environment Variable Buffer Overflow vulnerability.**
August 5, 2001	**Dbsnmp-8.1.6.C**	**Script which exploits the Oracle DBSNMP Oracle Home Environment Variable Buffer Overflow vulnerability.**
August 4, 2001	Tcptraceroute-1.2.tar.gz	An implementation of traceroute which uses TCP SYN packets, instead of the more traditional UDP or ICMP ECHO packets. In doing so, it is able to trace through many common firewall filters.
August 4, 2001	Nessus-1.0.8.tar.gz	A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems; it currently performs over 531 remote security checks.
August 3, 2001	**Nt4all.zip**	**Exploit for the Microsoft Windows NT 4.0 NT4ALL Denial of Service vulnerability.**
August 3, 2001	Scx-sa-21.txt	Globalscape's CuteFTP, a popular FTP client, uses a weak encryption scheme, allowing plaintext login and password recovery from the address book. Includes cuteftpd.c, which calculates the plaintext.
August 3, 2001	Nmap-2.54beta28.tgz	A utility for port scanning large networks, which supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
August 2, 2001	0107-exploits.tgz	New exploits for July, 2001.
August 2, 2001	**Evolut.C**	**Script which exploits the Oracle DBSNMP Oracle Home Environment Variable Buffer Overflow vulnerability.**
August 2, 2001	**Dbsnmpof.C**	**Script which exploits the Oracle DBSNMP Oracle Home Environment Variable Buffer Overflow vulnerability.**
August 1, 2001	**Locate-exploit.c**	**Script which exploits the GNU Locate Arbitrary Command Execution vulnerability.**
August 1, 2001	Ssh3.pl	SSH 3.0.0 vulnerability scanner.
August 1, 2001	Nsat-1.32.tar.gz	A fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine and much more.
July 31, 2001	**Sub7malphserver.sit**	**Subseven Macintosh Edition that allows Macs to be controlled from a PC and vice versa.**
July 30, 2001	**Arpkill.tar.gz**	**Script which exploits the Windows ARP Denial of Service vulnerability.**
July 30, 2001	Spadv03.txt	Technique for exploiting the Windows 2000 Telnetd vulnerability and includes SPtelnetAYT.c, a scanner for the AYT vulnerability in Telnet daemons build upon the BSD source.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 30, 2001	Lcrzosrc-3.15.tgz	A toolbox that contains over 200 functionalities and can be used to sniff, spoof, create clients/servers, create decode and display packets, etc.
July 29, 2001	Adore-0.39b4.Tgz	A Linux LKM based rootkit that features smart PROMISC flag hiding, persistent file and directory hiding (still hidden after reboot), process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine.
July 29, 2001	**Ibm-db2.c**	**Proof of concept Denial of Service exploit for the IBM DB2 vulnerability.**
July 29, 2001	Squidmap.pl	Squid can be used to port scan if set up as a httpd accelerator (reverse proxy).
July 29, 2001	_Root_040.zip	Windows NT Rootkit that hides processes, files, directories, has k-mode shell using TCP/IP and has a remote Telnet capability.
July 28, 2001	Asmcodes-1.0.2.pdf	Unix Assembly Code Development for Vulnerabilities Illustration Purposes v1.02 that covers IRIX / MIPS, Solaris, HP-UX, AIX, Ultrix, Linux, BeOS, and BSD systems.
July 28, 2001	Asmcodes-1.0.2.tar.gz	UNIX Assembly Codes Development for Vulnerabilities Illustration Purposes that includes sample assembly components for every discussed processor architecture.
July 27, 2001	Pic-lpr-remote.c	Exploit for the Pic / LPRng format string vulnerability.
July 25, 2001	**Agscrack.C**	**Script which exploits the FTP Server Weak Password Encryption vulnerability.**

Trends

Probes/Scans:

- **There has been an increase in scans of port 23 probing for the Multiple Vendor TelnetD vulnerability. (For more information, see the Multiple Vendor Telnetd Buffer Overflow vulnerability described above.)**
- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **The National Infrastructure Protection Center (NIPC) continues to work in close coordination with its public and private sector partners regarding what has been named Code Red II (See Virus Section). The NIPC considers Code Red II to be a serious threat because it spreads rapidly and installs a backdoor that can be accessed by anyone familiar with the exploit. For more information, see : NIPC ADVISORY 01-017 located at: http://www.nipc.gov/warnings/advisories/2001/01-017.htm.**
- **Microsoft has developed a tool that eliminates the obvious damage that is caused by the Code Red II worm. For more information, see "Tool to Remove Obvious Effects of the Code Red II Worm" available at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/redfix.asp.**
- **Internet backbone providers have notified the NIPC they are witnessing large-scale victimized web servers scanning for Microsoft Internet Information Server (IIS) vulnerabilities. The activity of the Code Red worm has the potential to degrade services running on the Internet. Any web server running the Microsoft IIS versions 4.0 or 5.0 that is not patched is susceptible to infection and exploitation as an attack platform. The NIPC is strongly urging consumers running these versions of IIS 4.0/5.0 to check their systems and install the patch. For more information, see NIPC ADVISORY 01-015, located at: http://www.nipc.gov/warnings/advisories/2001/01-015.htm or NIPC ALERT 01-016, located at http://www.nipc.gov/warnings/alerts/2001/01-016.htm. The Microsoft bulletin describing this vulnerability and its patch to fix the problem may be found at:**

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp **(also in CyberNotes-2001-13). Also see Trojan Section "TROJ_BADY.A."**

- **CERT/CC has received reports of W32/Sircam from over 300 individual sites. "W32/Sircam" is malicious code that spreads through e-mail and potentially through unprotected network shares. Once the malicious code has been executed on a system, it may reveal or delete sensitive information. (See Trojan Section). For more information, see CERT® Advisory CA-2001-22, located at: http://www.cert.org/advisories/CA-2001-22.html. Also see Trojan Section, "TROJ_SIRCAM.A."**
- **This year there has been a significant increase in activity resulting in compromises of home user machines. In many cases, these machines are then used by intruders to launch attacks against other organizations. For more information, see CERT® Advisory CA-2001-20, located at: http://www.cert.org/advisories/CA-2001-20.html.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

ce8.476: The virus is a small memory-resident, .com file-infecting virus that uses encryption on its virus code. Infected files have their file size increased by 476 bytes. The virus hooks Int. 21 in memory and infects .com files when they are run. The virus contains the following text within it:

*.COM
<CE-81>
v 1.1 by Geri$oft

CODERED.A (Aliases: TROJ_BADY.A, W32/Bady.worm, CODERED, CODE RED, HBC): This worm and its variant CODERED.B use a remote buffer overflow vulnerability in Internet Information Service (IIS) Web Servers that can give system-level privileges to a remote user, thereby compromising network security. This worm has two trigger dates and two payloads. The first payload is triggered when the current system date is between 20 and 28. The worm executes a Distributed Denial of Service attack (DDoS) on a government Web site (www1.whitehouse.gov). The second payload is triggered if the current system date is less than 20. The payload then executes and generates random IP addresses and sends copies of itself through port 80. IIS users should download Microsoft's patch for the .ida vulnerability.

End_of.566 (DOS Virus): This is an older DOS virus that infects .com files. It is not memory-resident. If the year is 2000 or later, the virus displays a message every time that it is activated.

HLLO.True (DOS Virus): This virus is a DOS overwriter that is written in Pascal. It overwrites all .exe files in the folder that contains the virus.

VBS.Ave.A (Visual Basic Script Worm): This is a Visual Basic Script virus. When it is executed, it infects .vbs or .vbe files that are in the folder that contains the virus.

VBS/Haptime-A (Aliases: VBS/Help, Happy Time, VBS/Haptime@MM) (Visual Basic Script Worm): This worm has been reported in the wild. It is a worm that spreads via Outlook Express version 5.0. It attempts to infect files with the extensions VBS, HTML, HTM, HTT and ASP. It will also attempt to delete EXE and DLL files when the month plus the day are equal to 13 (for instance, June the 7th).

VBS.Noon (Alias: I-Worm.Noon) (Visual Basic Script Worm): This is a typical VBS worm that uses Microsoft Outlook MAPI to mail itself out to all contacts in the e-mail address book. One notable difference though lies in how this worm reacts to different mailer programs installed on the computer. When this worm is activated it deletes the file C:\Windows\Rundll32.exe. This path name is hardcoded in the virus. Depending on which e-mail client you are using at the time, the virus will then do one of two things: If you are using Microsoft Outlook, this worm will create copies of itself on your C drive with the following names (the path and file names are hard-coded in the worm):

C:\Wormmie.vbs
C:\Wormmie.bat
C:\Wormmie.ini
C:\Wormmie.pif
C:\Program Files\Wormmie.vbs
C:\My Documents\Wormmie.vbs

The virus also creates the following file in your \Windows\System folder:

%System%\Wormmie.vbs

(NOTE: %System% is a variable that identifies the location of your \Windows\System folder.) The file Wormmie.vbs is used by the worm to send itself out to all the contacts in your Microsoft Outlook Address Book. While going through your contact list, this worm displays a message box with the e-mail address of each contact that is sent a copy of the worm. After e-mailing each contact, this worm will create the following registry key, which it sets to the value of 1:

HKEY_CURRENT_USER\software\An\mailed

If you are using a e-mail client other than Microsoft Outlook, this worm will display the series of message boxes. If the registry key HKEY_CURRENT_USER\software\ An\mailed is set to 1, the worm displays the following message, "You already auto send the Virus to everyone." If the registry key HKEY_CURRENT_USER\software\An\mailed is not set to 1, the worm displays the following message, "Too bad! Not infected yet! Keep trying…" Finally the worm does a time check to see if the time is equal to 00:00:00 or 12:00:00. If the time is equal to 00:00:00 it displays the following message, "Dong! Dong! Dong! Is already mid-night and I'm your worst nightmare"! If the time is equal to 12:00:00 the worm displays the following message, "Is noon and let's have lunch together." Following the e-mail program-dependent actions, the worm opens one of three Internet search engines. Finally the worm displays a message box with the following text:

Wormmie
Wormmie! Wormmie! Wormmie! Wormmie! Wormmie! Wormmie!

VBS/PeachyPDF-A (Variants: VBS/PeachyPDF-B, VBS/PeachyPDF-C) (Visual Basic Script Worm): This worm uses a feature in the full version of Adobe Acrobat to execute its code from a PDF file. The PDF file will arrive by e-mail and the subject will contain one of the following:

"You have one minute to find the peach"
"Find the peach"
"Find"
"Peach"

The text of the message will be one of the following:

"Try finding the peach"
"Try this"
"Interesting search"
"I don't usually send this things, but..."

The attachment will be called one of the following:

"find.pdf"
"peach.pdf"
"find the peach.pdf"
"find_the_peach.pdf"
"joke.pdf"
"search.pdf"

When the user opens the attachment, a PDF with the title "You have one minute to find the peach" is displayed. If the user follows the instructions in the PDF, using the full version of Acrobat, Acrobat will extract the worm and run it. It will display an image with the text "Line1,picture6" while it is using Outlook to mail itself out.

VBS/Potok-A (Visual Basic Script Worm): This is an e-mail-aware worm, which uses Microsoft Outlook to spread itself. The worm sends an e-mail to the first 50 addresses in the Outlook address book with the following characteristics:

Subject line: "New Generation of drivers."
Message body: "Microsoft has published new driver for all types Video Cards, compatible with Windows 95/98/NT/2000/XP. You can read about it in attachment document. Best wishes, Microsoft."
Attached filename: "\driver.doc***.vbs" (where *** represents 46 spaces)

Please note that this file name has 46 spaces before its final .vbs extension in an attempt to fool users into thinking it is a Word document. On a Windows NT machine using the NTFS filing system, the virus will hide part of its code in the Alternate Data Streams associated with the file ODBC.INI in the Windows subdirectory.

VBS.Merlin.C@mm (Visual Basic Script Worm): This is a mass-mailing worm written in the Visual Basic Scripting (VBS) language. The worm spreads by e-mailing itself to all contacts in the Microsoft Outlook address book. It can also spread across network drives and by using an IRC client and Gnotella (a client used on the Gnutella network). Its main payload attempts to create 10,000 randomly named folders in the root of drive C and places a text file into each of these folders.

VBS.Millennium (Visual Basic Script Worm): VBS.Millennium is a simple Visual Basic script worm that spreads using mIRC. It displays the message: !!HAPPY NEW MILLENNIUM!!.

W32.Annoying.Worm (Win32 Worm): This worm is a Visual Basic 6 (VB6) program that spreads using MSN Messenger. It requires Msvbvm60.dll to run.

W32/Choke (Aliases: I-Worm.Choke, Win32.Choke, W32/Choke.Worm) (Win32 Worm): This worm has been reported in the wild. It attempts to send itself through the MSN Messenger instant messaging program. The worm can send itself through MSN Messenger using a variety of filenames, including ShootPresidentBUSH.exe and Choke.exe. It copies itself to c:\choke.exe and sets a Registry key HKCU\Software\Microsoft\Windows CurrentVersion\Run\Choke in order to run automatically when Windows is started. When first executed the worm displays two dialog boxes. The first dialog box says:

"This program needs Flash 6.5 to run!"

The second displays the message:

"Cannot run program!, Quitting"

W32/Hai.worm (Alias: Win32.Hai (CA)) (Win32 Worm): This worm simply spreads using open network shares via NetBios. When run, it begins scanning the entire local Class A subnet, looking for any open shares. If one is found, the worm tries to copy itself the Windows directory (using a random filename) on that machine and create a WIN.INI RUN value to load itself at startup.

W32/Hybris-F (Win32 Worm): This is a worm capable of updating its functionality over the Internet. It consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects WSOCK32.DLL. Whenever an e-mail is sent, the worm attempts to send a copy of itself as an attachment to a separate message to the same recipient. Any other behavior exhibited by the worm is entirely dependent on the set of installed components. The text of the e-mail message is determined by one of the installed components, and hence can be changed by the upgrading mechanism detailed below. Consequently the message can have any subject, any message text and any filename for the attached file. A common component of the worm checks the language settings of the computer it has infected, and selects a message accordingly from: English, French, Portuguese, and Spanish. The methods for upgrading the worm can also be changed as they are also upgradeable components. At the time of writing, two have been seen. One of the upgrading

techniques attempts to download the encrypted components from a website, which is presumably operated by the worm author. This website has since been disabled. However, this component could be upgraded to have a different web address. The other method involves posting its current plug-ins to the Usenet newsgroup alt.comp.virus, and upgrading them from other posts by other infections of the worm. These are again in the encrypted form, and have a header with a four character identifier and a four character version number, in order for the worm to know which plug-ins to install. Another component of the worm searches the PC for .ZIP and .RAR archive files. When it finds one, it searches inside it for an .EXE file, which it renames to .EX$, and then adds a copy of itself to the archive using the original filename. There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour on any day in the year 2001, displays a large animated spiral in the middle of the screen that is difficult to close. There is also a component that applies a simple polymorphic encryption to the worm before it gets sent by e-mail. By upgrading this component the author is able to completely change the appearance of the worm in unpredictable ways in an attempt to defeat detection by anti-virus products.

W32/Linong-A (Alias: VBS/Linong-A) (Win32 Worm and Visual Basic Script Worm): This is an e-mail-aware worm which sends itself in an e-mail message with the subject line randomly chosen. When the attached file is run it drops a VBS file which attempts to send the file to all contacts in the Microsoft Outlook address book. The worm also creates 501 directories in the root of the C: drive. The directories are named "Linong I Love U So Much Linong For ever My Love<number>" where <number> is an integer between 0 and 500 inclusive. When the date is June 25 the worm displays a message box containing the text:

"Happy Birthday To MyLinong
Still Remember Me..."

On July 22 the worm displays a message box with the text:

"Today I want tell you Once again that
I LOVE YOU SO MUCH LINONG
Hey user, Please Help me to Tell the world
That I love Her So Much"

On November 14 the worm displays a message box with the following text:

"Hi..Nong..I Love You So much.
But today we must Say GoodBye For ever
I wait U in the next Life and Remember I Love You so Much"

W32/Parrot-A (Aliases: W32/Crackly@MM, I-Worm.Parrot, W32/Parrot@MM) (Win32 Worm and Companion Virus): This virus has been reported in the wild. It is an e-mail-aware worm and companion virus. The worm arrives in an e-mail with the subject line "Parrot screensaver." The body of the e-mail message contains the text "Hehe hey, look at this screensaver :)." The infected attached filename is called parrot.scr. The worm attempts to send itself to all contacts in the Microsoft Outlook address book, and drops a mIRC (Internet Relay Chat) script which will attempt to send the worm file C:\parrot.scr to other mIRC users. The companion virus renames files in the Windows directory, renaming .EXE files to .PRT (for instance, calc.exe to calc.prt) and copies itself to the original filename. The virus also drops an audio file that is opened and played when the virus is run. Furthermore, the virus drops a VBS file that displays a message box containing offensive text about anti-virus researcher Graham Cluley. The virus changes the following registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

so that the dropped audio file is opened and the dropped VBS script is run on Windows startup.

W97M.Ethan.DE (Alias: Macro.Word97.Ethan.dp) (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the Normal.dot file. It creates the file C:\Winsys.log, which contains the source of the virus. The virus uses this file to copy the viral code into an uninfected document. The virus randomly generates a number between 1 and 10. If the computer date is the year 2001 or later and the randomly generated number is 5, the virus adds the following lines to the C:\Autoexec.bat file:

```
@echo
@echo y|format c:/q/u >nul
```

When the computer is restarted, the Autoexec.bat file runs the additional lines and formats drive C.

W97M.Inspector.E (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. This virus infects documents when they are created, opened, or closed. If the virus finds that an older version of itself is installed, it deletes the older version and replaces the code with the current version.

WM97/Cruson-A (Word 97 Macro Worm): This is an e-mail-aware worm. The worm sends itself as a copy of the infected active Microsoft Word document to all addresses in the user's Outlook address book. The subject line of the e-mail is "From " followed by the Word application username (for instance, "From John Smith"). The body text of the e-mail reads: "I remembered something last night. It is very, very important document. Look in attachment."

X97M.BDoc2 (Excel 97 Macro Virus): This is an Excel macro virus that infects the active workbook and inserts an infected workbook in the \XLStart folder. It is activated when opening, closing, or saving a file, and when Excel starts or exits. However, it only infects workbooks when files are opened, closed, or saved. When this virus is activated, it disables:

Macro virus protection in Excel.
The display of alerts when a modified workbook is saved.
Screen updating. The modifications are not displayed; this is done to hide its activities.

The virus infects the active worksheet by creating the module Bdoc2, into which it inserts itself.

X97M_DIVI.L (Aliases: DIVI, DIVI.L) (Excel 97 Macro Virus): This virus has been reported in the wild. It infects ThisWorkbook modules of target Excel files. The virus triggers whenever an infected file is opened. It has no destructive payload. When an infected file is opened, this virus copies and installs itself to a BOOK1.XLS file in the Excel startup directory and intercepts the automacro Workbook_Open. Thereafter, it infects by inserting its codes into Excel files that are opened. This virus does not re-infect previously infected files.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.IRC.Flood	**N/A**	**Current Issue**
Backdoor.MiniCommander:	**N/A**	**Current Issue**
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	**N/A**	**Current Issue**
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
BAT.Install.Trojan	N/A	CyberNotes-2001-04
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	**II**	**Current Issue**
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.StartPage	N/A	CyberNotes-2001-07
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	**N/A**	**Current Issue**
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/PsychwardB	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWSAGENT.A	**N/A**	**Current Issue**
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10

Trojan	Version	CyberNotes Issue #
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	**N/A**	**Current Issue**
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	**N/A**	**Current Issue**
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	**N/A**	**Current Issue**
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Natas	**N/A**	**Current Issue**
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
Y3K Rat	1.6	CyberNotes-2001-11

Backdoor.IRC.Flood (Aliases: Backdoor.IRC.Flood.i, Backdoor.IRC.Flood.f): This is a backdoor Trojan. It installs a mIRC client that has backdoor capabilities; this gives an attacker unlimited access to the computer.

Backdoor.MiniCommander: This is a backdoor Trojan that copies itself to the \Windows folder as Trdrv98. After it does that, it creates an entry in the System.ini file that causes Trdrv98 to run when Windows starts.

Backdoor.Teste: This is a backdoor Trojan that is written in the Visual Basic (VB) language. This program sends an e-mail message to the attacker and gives him or her unrestricted access to the victim's computer. The installation package of this backdoor Trojan creates the folder C:\~setup.t on the computer. It then creates the following files in the folder:

C:\~setup.t\Teste.exe
C:\~setup.t\Mswinsck.ocx

The Trojan then executes Teste.exe, which copies Teste.exe and Mswinsck.ocx to the following (hardcoded) locations as:

C:\Windows\Netcom1.exe
C:\Windows\System\Mswinsck.ocx

Teste.exe also creates the value modem1 with the value data C:\WINDOWS\NETCOM1.EXE in the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Finally, Teste.exe executes the new copy of itself (Netcom1.exe), which sends an e-mail message to the attacker and provides the backdoor functionality.

CodeRed II (Aliases: CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C): CodeRed II was discovered on August 4, 2001. It has been called a variant of the original CodeRed Worm because it uses the same "buffer overflow" exploit to propagate to other Web servers. CodeRed II is considered to be a high threat and has been reported in the wild. The original CodeRed had a payload that causes a Denial of Service attack on the White House Web server. CodeRed II has a different payload that allows the hacker to have full remote access to the Web server. The worm propagates by installing itself into a random Web server using a known buffer overflow exploit, contained in the file Idq.dll. Only systems that have not been patched with the latest Microsoft IIS service packs can be affected. Microsoft has published information on this vulnerability and a Microsoft patch is available at: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp. When a Web server is infected, the worm will first call its initialization routine, which identifies the base address of Kernel32.dll in the process address space of the ISS server service. Next it looks for the address of GetProcAddress. Then it starts to call GetProcAddress to get access to a set of API addresses:

LoadLibraryA
CreateThread
GetSystemTime

It then loads WS2_32.dll to access functions such as socket, closesocket and WSAGetLastError. From USER32.DLL, it gets ExitWindowsEx that is used by the worm to reboot the system. The main thread checks for two different markers. The first marker, '29A', controls the installation of the Trojan.VirtualRoot. The other marker is a semaphore named 'CodeRedII'. If the semaphor exists, the worm goes into an infinite sleep. Next, the main thread checks the default language. If the default language is Chinese (either Taiwan or PRC), it creates 600 new threads, otherwise it creates 300. These threads generate random IP addresses used to search for new Web servers to infect. While these threads are working, the main thread copies Cmd.exe from the Windows NT \System folder to the following folders (if they exist).

C:\inetpub\Scripts\Root.exe
D:\inetpub\Scripts\Root.exe\
C:\progra~1\Common~1\System\MSADC\Root.exe
D:\Progra~1\Common~1\System\MSADC\Root.exe

If the Trojan that is dropped by the worm has modified the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\W3SVC\Parameters\Virtual Roots

(by adding a few new keys and setting the user group to 217), it allows an attacker to take full control of the Web server by sending an HTTP GET request to run scripts/root.exe on the infected Web server. The main thread sleeps for 48 hours on Chinese systems and for 24 hours on other systems. The 300 or 600 threads will still work and attempt to infect other systems. When the main thread wakes up from its sleep, it will cause the computer to be rebooted. In addition, all threads check if the month is October or if the year is 2002. If so, the computer is rebooted. It will also drop a file that has its attributes set to hidden, system and read-only onto the root drive as either or both C:\Explorer.exe or D:\Explorer.exe. The worm carries this files inside itself in a packed format and unpacks it when it's dropped. The infection will last 24 or 48 hours and then the computer will be rebooted. However, the same computer can be infected again until it is patched with the latest update from Microsoft. When the computer is rebooted, Trojan.VirtualRoot will be executed when the system attempts to execute Explorer.exe, due to how Windows NT resolved or searches the program path when executing a program. The Trojan (C:\Explorer.exe) will sleep for a few minutes and reset these keys to assure that the registry keys are modified. It should be noted that after a reboot the memory resident worm will be inactive. This means that on an infected system which has been rebooted, the worm will not attempt to spread itself to other machines unless it happens to get reinfected. The Trojan also alters the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

so that the value of SFCDisable is set to 0xFFFFFF9D. This disables the System File Checker (SFC).

KillMBR.g: This is a Trojan horse that overwrites the Master Boot Record (MBR) with zeroes.

Trojan.Bat.Live4: This is a Trojan horse that attempts to delete system files, files on drive A, and .doc files that are in the C:\My Documents folder.

TROJ_NEWSAGENT.A (Aliases: NEWSAGENT, NEWSAGENT.A, Flooder.NewsAgent): This Win32 Trojan hacking tool named NewsAgent by HipCrime, is a mail management system for Usenet. The Trojan enables a remote user to post messages, cancel messages, undelete messages canceled by other network users, replace posted messages, and create new Usenet groups even without news administrator privileges. It also allows its user to flood newsgroups with numerous messages.

Trojan.VirtualRoot: This is a Trojan horse program that is dropped by the CodeRed II worm. The Trojan allows a malicious remote user to have full remote access to the Web server that is infected by CodeRed II. If Trojan.VirtualRoot has modified the registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Services\W3SVC\Parameters\Virtual Roots

(by adding a few new keys and setting the user group to 217), it allows the attacker to take full control of the Web server by sending an HTTP GET request to run scripts/root.exe on the infected Web server.

VBS.AutoExec.Trojan (Alias: Bloodhound.VBS.Threat): This is a Visual Basic Trojan that modifies the C:\Autoexec.bat file. The next time that the infected computer is restarted, the following files are deleted:

C:\Windows\System*.*
C:\Windows*.*
C:*.*

VBS.Natas (Alias: VBS.Lucky2): VBS.Natas is a Visual Basic Script (VBS) Trojan/worm that overwrites all files that are in the same folder as the virus. When this script is executed, it searches the current folder for files and overwrites them with itself. Then it randomly picks a number (1 or 2). If it picks the number 1, it displays the message:

"SEEK REFUGE FOR SATAN HOLDS NO MERCY FOR THE WEAK THE SICK AND UNWANTED!"

Next it creates the file C:\Windows\Favorites\Natas.url and adds a link to a Web site to the newly created file. Finally, it runs the Natas.url file, which opens your Web browser and attempts to connect to the linked-to site.